4

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,716	01/31/2001	Masayuki Chatani	375.07.01	7005

25920	7590	02/22/2005

MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _24 August 2004_ .

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _12-27 and 54-87_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _12-27 and 54-87_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on _31 January 2004_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1.   In response to communications filed on 8/24/2004, applicant cancels claims 1-11 and 28-

53, amends claims 12, 14, 20, 22, 23, 24, and 27; applicant also adds claims 54-87. The

following claims 12-27 and 54-87 are presented for examination.

1.1   Applicant's arguments, pages 16-18, filed on 8/24/2004, with respect to the rejection of

claims 1-57 have been fully considered, but they are not persuasive. Applicant amends

independent claims 12 and 22 to include the word ID as the user identifier. Regarding claim 12,

Applicant argues that Uranaka does not teach a detachable storage medium having a data

structure including a user identifier and argues that Uranaka does not teach a server that encrypts

the software product using the user identifier and a purchase option, then alleges that Uranaka

teaches to encrypt the distributed application package by key Kv encrypting with a user key Pku,

but the user public key PKu is not tied to any user. Examiner respectfully disagrees because the

Pku is tied to the user at the time of applying for the service (column 7, lines 5-10). Uranaka

(column 2, lines 60-67) teaches a user ID code which is recorded on a DVD that meets the

recitation of a detachable storage medium having a data structure including a user identifier.

Uranaka teaches a detachable storage medium having a data structure comprising at least one of

a user identifier ("the combination of VID and NOv-i serves as user ID of the application

package or DVD" and further discloses member ID, name and address are also associated with

each record (column 5, line 57 through column 6, line 5 and column 7, lines 58-67; see also

summary column 2, lines 20-67 (emphasis added)). Uranaka also discloses encrypting each

product using information comprising user identifier and purchase option (column 14, lines 1-37). Uranaka also discloses that the limit value is included in the package and added to the VID and NOv-i that also serves as user ID (column 13, lines 38-40).

Regarding claim 22, Applicant also argues that the client does not send any encrypted information to the server. Applicant respectfully disagrees. First, claim 22 discloses a decryption module for receiving decryption information from the user not for receiving encrypted information. Second, Uranaka discloses: (column 12, lines 15-25) cites "the client sends the encrypted data to the server... the server decrypts the received encrypted data with the server key". See also figure 20c for other encryption/decryption exchange between client and server. For at least the reasons cited above, Applicant has not overcome the rejection in view of the amended claims. Therefore, claims 12-27 remain rejected on the same ground of rejection and are not patentable over Uranaka. The dependent claims to claims 12 and 22 not challenged New claims 54-87 are rejected under 35 USC 102 in view of Richards et al.

Specification

2.   The amendment filed 8/24/2004 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: "At the user side, the user will use the user public key (User A) to decrypt the user private key (User B) and the console private key (Console B) to decrypt the console public key (Console A)." Figure 2B does not show either the added material.

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Objections

3.   **Claims 22, 81, and 82** and the intervening claims are objected to because of the

following informalities: the term "adapted to" is not a positive limitation and should be

corrected. Appropriate correction is required. See MPEP § 2106.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999

(AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002

do not apply when the reference is a U.S. patent resulting directly or indirectly from an

international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA

35 U.S.C. 102(e)).

4.1   **Claims 12-27** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent

6,470,085 to **Uranaka et al.**.

4.2   **As per claim 12, Uranaka et al.** discloses a system for providing access to restricted use

of digital software products, a server network comprising a server computer, a customer database

storing user information, and a content database storing a plurality of software product titles, for

example (see column 7, line 58 through column 8, line 42); a client console, operated by a user

and configured to playback a selection of the plurality of software product titles, for example

(see column 7, lines 10-37), a detachable storage media installable in said client console, for

example (see column 7, lines 10-37); said detachable storage media having a data structure

thereon comprising at least one of a user identifier (ID) (column 5, line 57 through column 6,

line 5 and column 7, lines 58-67; see also summary column 2, lines 20-67), wherein the server

computer distributes a software product to a user of the client console and encrypts the software

product using information comprising the user identifier and a purchase option governing use of

the software product by the user, for example (column 5, line 57 through column 6, line 5 and

column 7, lines 58-67; see also summary column 2, lines 20-67 (emphasis added)). Uranaka also

discloses encrypting each product using information comprising user identifier and purchase

option (column 14, lines 1-37), Uranaka also discloses that the limit value is included in the

package and added to the VID and NOv-i that also serves as user ID (column 13, lines 38-40)

that also meets the recitation of wherein the server distributes a software product to a user of the

client console and encrypts the software product using information comprising the user identifier

and a purchase option governing use of the software product by the user.

As per claim 22, Uranaka et al. discloses a server computer coupled to one or more

client computers over a communications network, the server computer comprising: a customer

database storing user information and a content database storing a plurality of software product

titles to a user of a client computer of the one or more client computers upon request of the user,

for example (see column 7, line 58 through column 8, line 42); Uranaka also discloses

encrypting each product using information comprising user identifier and purchase option

(column 14, lines 1-37). Uranaka also discloses that the limit value is included in the package

and added to the VID and NOv-i that also serves as user ID (column 13, lines 38-40) that meets

the recitation of an encryption module encrypting the software product using information

comprising a user identifier and a purchase option governing use of the software product by the

user (column 2, lines 20-67 and column 5, line 57 through column 6, line 5 and column 7, lines

58-67); and a decryption module receiving decryption information from the user and providing

access to the software product upon confirmation of the decryption information, for example

(column 12, lines 15-25).

As per claim 13, Uranaka et al. discloses the limitation of wherein the user transmits

decryption information to the server computer to provide access to the software product

distributed to the user, for example (see column 2, line 62 through column 3, line 6 and column

6, line 41 through column 7, line 20).

As per claim 14, Uranaka et al. discloses the limitation of wherein the software product is distributed to the user on a readable disk media, for example (see column 6, line 41 through column 7, line 20).

As per claim 15, Uranaka et al. discloses the limitation of wherein the server computer distributes the software product to the user over a communications link coupling the client computer to the server, for example (see column 4, line 44 through column 5, line 56).

As per claims 16, 17, 26, and 27, Uranaka et al. discloses the limitation of wherein the user transmits the decryption information to the server computer using a telephone coupled to the server computer through a public switched telephone network, for example (see column 6, line 41 through column 7, line 20 and column 4, lines 44-65).

As per claims 18, 19 and 23, Uranaka et al. discloses the limitation of, wherein the software product purchase option comprises one of purchasing the software product for a bounded period of time or purchasing the software product for a preset period of accesses and a preset number of accesses, for example (see column 6, lines 6-42 and column 14, lines 1-13).

As per claims 20 and 24, Uranaka et al. discloses the limitation of wherein the software product is encrypted using a public key/private key encryption system, and wherein a user public key is assigned and transmitted to the user and a client console public key is assigned and coded

in the detachable storage media installable in the client console, for example (see column 14, line

14-27 and column 1 6, lines 13-45 and column 11, line 40 through column 12, line 25).

As per claims 21 and 25, Uranaka et al. discloses the limitation of wherein the client

console is an interactive computer game station and the software product is a computer game

executable on the client console, for example (see column 4, line 44 through column 5, line 5).

5.   **Claims 54-79 and 81-86** are rejected under 35 U.S.C. 102(e) as being anticipated by US

Patent Publication US 2002/0016922 to **Richards et al.**

5.1   **As per claims 54, 65, 74, and 81, Richards et al** discloses a method for distributing a

software product, comprising the steps of: an article of manufacture embodying a program of

instructions executable by a machine, the program of instructions configured and adapted for

execution on a client console or remote server, the article of manufacture including instructions

for: encrypting said software product (page 4, paragraph 0061); distributing said encrypted

software product to a user (page 4, paragraph 0061); receiving an encrypted software product

(page 4, paragraph 0061); **Richards et al** discloses establishing two-way communication

between a server and remote apparatus of a user using public key/private key encrypted, secure

communication that meets the recitation of establishing, in conjunction with a reception of

counterpart communication originating from a remote content provider server or remote

apparatus (page 7, paragraph 0092), two-way, public key/private key encrypted, secure

communication between said content provider server and said client console (page 8, paragraphs

0096-0097); **Richards et al** discloses receiving keys for decryption of said encrypted software

product from said content provider server that meets the recitation of receiving, via said secure

communication, data (Title B) enabling decryption of said encrypted software product from said

content provider server (page 7, paragraph 0093).

As per claims 55, 66, 75, and 82, Richards et al discloses the limitation of

communicating purchase information from said user to said product distributor (page 8,

paragraph 0103); and communicating, responsive to said purchase information and via said

secure communication, an electronic token from said product distributor to said user that permits

said user to use said decrypted software product in a restricted manner, for example (page 8,

paragraph 0096).

As per claims 56, 67, 76, and 83, Richards et al discloses the limitation of wherein said

use in a restricted manner constitutes use for a bounded period of time or use for a predetermined

number of usages (page 1, paragraph 0004).

As per claims 57, 68, 77, and 84, Richards et al discloses the limitation of wherein said

data enabling decryption of said encrypted software product is a private key (Title B) of a first

public key/private key pair that is separate from the public key/private key pairs of said secure

communication (page 8, paragraph 0097).

As per claims 58 and 69, **Richards et al** discloses the limitation of wherein the dynamic key that enables decryption is private key of one of the exchanges of public key/private key pair encoding schemes that meets the recitation of wherein the dynamic key that enables decryption is private key from a said data enabling decryption of said encrypted software product is a private key of said first public key/private key pair (page 8, paragraph 0097).

As per claims 59, 71, 79, and 86, **Richards et al** discloses receiving a public key, unique key from the server and generating a third public/private key pair and using that key to encrypt a third public key (machine key) and communicating said encrypted third public key to said content provider server (page 8, paragraph 0097) and a final key set for future encoding/decoding that meets the limitation of wherein said establishing of secure communication comprises: receiving, as said counterpart communication, a public key of a second public key/private key pair (User A, User B) from said content provider server; generating a third public key/private key pair (Console A, Console B); encrypting said third public key using said second public key; and communicating said encrypted third public key to said content provider server; and decrypting said encrypted third public key using said second private key.

As per claim 60, **Richards et al** discloses in one embodiment a user unique browser ID is provided to the server from the remote apparatus to create public key/private key pair that meets the limitation of wherein said second public key/private key pair is created using user information (ID) provided by said user to said product distributor (page 8, paragraph 0096). In

another embodiment, **Richards et al** discloses a user unique ID is provided to the server from

the user to create keys for encoding/decoding that also meets the limitation of claims 60 and 61

(page 11, paragraph 0130-0131).

As per claim 61, Richards et al discloses using unique machine identifier to generate

key set that meets the recitation of wherein said third public key/private key pair is created using

hardware identification means, a hardware identification device or a media identifier of a

medium on which said encrypted product has been distributed (page 8, paragraph 0096).

As per claim 62, Richards et al discloses software product that is user and apparatus

specific for execution that meets the recitation of wherein an execution of said software product

on a user's computer requires connection of said hardware identification device to said user's

computer (page 9, paragraph 0105-0106).

As per claims 63, 64, 70, 72, 73, 78, and 85, Richards et al discloses the limitation of

wherein any of said communication or said secure communication from said user to said product

distributor is effected via touch-tone signals or voice over a public switched telephone network

and wherein any of said communication or said secure communication from said product

distributor to said user is effected via voice synthesis or voice over a public switched telephone

network (page 4, paragraph 0061).

Claim Rejections - 35 USC § 103

6.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or

described as set forth in section 102 of this title, if the differences between the subject matter

sought to be patented and the prior ail are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which

the invention was made.

6.1   **Claims 80 and 87** are rejected under 35 U.S.C. 103(a) as being unpatentable over US

Patent Publication US 2002/0016922 to **Richards et al** in view of US Patent 5,490,216 to

Richardson, 111.

6.2   **As per claims 80 and 87, Uranaka et al.** substantially teaches the claimed method and

article of manufacture of claims 74 and 81. **Richards et al** discloses securely distributing

encrypted data using any communication protocol including the Internet for communicating

encrypted information between a server and a user, but does not explicitly disclose wherein said

secure communication comprises displaying said encrypted public key on a display device.

Richardson, III in an analogous art teaches distributing protected data using secure

communication wherein said secure communication comprises displaying said encrypted public

key on a display device, for example (see column 7, lines 1-7). Therefore, it would have been

obvious to one of ordinary skill in the art at the time the invention was made to modify the

method of **Richards et al** to display said encrypted public key on a display device so that the

registration process can be done in real time with the server in this manner the registration

procedure ensures that exactly the same information entered by the user on his/her PC are those

recorded by the server (column 7, lines 35-67). This modification would have been obvious

because one skilled in the art would have been motivated by the suggestions provided by

Richardson, III so that the registration process can be done in real time with the server in this

manner, the registration procedure ensures that exactly the same information entered by the user

on his/her PC are those recorded by the server (column 7, lines 35-67).

Conclusion

7.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

7.1   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.
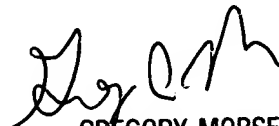
Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Carl Colin

Patent Examiner

February 7, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100